

Information Services Board Briefing Paper on Statewide Information Technology Security Policy and Status of Agency Security Program Compliance Letters

Prepared by Mary Lou Griffith, DIS/MOSTD, (360) 902-2978.

Description

Digital government requires a secure and trustworthy environment for conducting sensitive transactions through open networks. To that end, the Information Services Board (ISB) initiated a comprehensive review and update of the statewide Information Technology (IT) Security Policy to address the security issues of conducting electronic commerce across the state enterprise. The IT Internet Security Program Charter was developed and approved at the June 12, 2001, ISB meeting. A recommendation that an Independent Security Analyst be assigned to report the status of the state's IT Security Program on a recurring basis was also approved by the Board at that time. Mr. Jeff Scheel was named as the ISB Independent Security Analyst and will report the current status of the IT Security program to the Board.

Background

Washington State government has been recognized as a leader in applying digital technologies and the Internet in service to the citizen. This has been achieved by leveraging the open architecture of the Internet to provide access to a wide range of public information and services.

Using the Internet to its greatest advantage requires a higher degree of security than was the case in an earlier era of closed systems and proprietary networks. Washington State government must take sufficient steps to ensure that citizens and businesses interacting with public agencies are protected by the appropriate information technology security. Beyond a range of anonymous exchanges available through the Internet, citizens and businesses need secure access to look up their medical or other benefit claims, exchange sensitive health records, and make or receive electronic payments with government. All these transactions require secure access control and data protection for the electronic exchange of information over the Internet. This is being done through the state's secure gateway, Transact Washington, which implements trustworthy access control through Public-Key Infrastructure (PKI).

Washington State government has set a clear direction and minimum standards for the way in which sensitive information and transactions must be protected by state agencies. The policies, standards, and guidelines set the preconditions for achieving a consistent and reliable set of protections for sensitive information within a shared, trusted environment.

Status

The annual compliance letter regarding their respective information technology security programs was due from each agency head on August 31, 2002. Agencies were advised that the annual security program verification should be an accurate reflection of the agency's compliance with the policy and that the ISB was interested in agency progress towards full compliance. The letters were to address the following topics:

- A statement that the agency is in compliance or working towards it
- A date when the agency expects to reach full compliance
- A list of accomplishments
- A list of remaining tasks

A draft charter was prepared and the Architecture Sub-Committee of the Customer Advisory Board was invited to participate and complete the charter for the establishment of the Washington Computer Incident Reporting Center (WACIRC). WACIRC has been meeting weekly to discuss improved incident prevention, response, and methods for information sharing. They are in the process of developing a state incident response plan.

A list of agencies that completed their letter and an analysis of the results will be presented to the ISB at the October 9, 2002 ISB meeting.

Issues

- Some agencies have reported difficulties in fully implementing their security plans due to budget issues.
- Additional assistance may be needed for the implementation of effective Security Awareness Training. DIS has contracted for an online Security Awareness training course and plans to make it available at no cost to agencies that have access to Inside Washington.

Recommendation

DIS recommends that the ISB continue to receive reports from the DIS staff and the ISB Independent Security Analyst on the status of agency security program review and statewide efforts to address information technology security issues.